IOSPHERE

China's Comprehensive IW-Strategy Link

By Timothy L. Thomas

Editorial Abstract: *Mr. Thomas describes how China's Internet reconnaissance capability is central of establishing the strategy of "winning victory before the first battle." Associated actions include China's focus on collecting technical parameters of other systems from which Chinese specialists develop countermeasures. A review of current Chinese IO theory reinforces their preemptive cyber strategy policy.*

Introduction

Information operations offer the Peoples Liberation Army (PLA) a new vector for the Chinese military's transformation from an industrial to a modern day force. Recent Chinese White Papers on national defense describe this vector as the requirement to informationize the armed forces. The 2006 White Paper, for example, states the RMA is developing worldwide and, based on informationization, military competition is intensifying. This document adds that informationization will be used as the main criteria to measure the qualitative improvement of the PLA; that for China to build a strong defense, it must build informatized armed forces and be capable of winning informatized wars by the middle of the twenty-first century; and that the PLA has built virtual laboratories, digital libraries, and digital campuses to support the training and teaching needed to field this informatized force.

How IO Has Changed in China over the Past Few Years

The basic definition of information operations has evolved slowly over the past ten years. Only two of scores of definitions will be discussed here, albeit two proposed by very influential people in the Chinese IO arena. In 1999, IO specialist Yuan Banggen stated that information operations are specific information warfare (IW) operations. He added that IW is the core of informationized warfare, whereas information operations are the manifestation of information warfare on the battlefield; that IO means information wars in the narrow sense, that is the military field; and that IO includes integrated, high technology countermeasures. According to Yuan,

People's Liberation Army flag. (Wikimedia)

IO's theoretical system is formed from two levels, basic and applied. Basic theories consist of concepts such as its organizational structure and technological equipment, command and control for IO, and so on. He categorizes applied theories into offensive IO and defensive IO; strategic, operational, campaign, and tactical levels; and into peacetime, wartime, and crisis-period IO. IO's two missions are preparation and implementation. Yuan notes that principles are centralized command, multi-level power delegation, multi-dimensional inspection and testing, timely decision-making, and the integration of military and civilian actions with a focus on key links. Overall, Yuan states that all activities of IO focus attention on command and control.

A 2005 book, *Study Guide for Information Operations Theory*, offers several definitions of IO, and these have progressed over time. Dai Qingmin, an IO specialist and former chief of a General Staff Directorate, and his co-workers note:

At present there are three main definitions for information operations. The first is as follows: 'Information operations refer to operations used to gain and maintain control over information.' This definition expands the domain of information operations, as there are quite a few ways to gain and maintain control over information. Second, 'Information operations refer to a series of operational actions employed by two sides in a conflict in which the enemy's information systems are used or destroyed and one's own information systems are protected as a means of gaining the power to acquire, control, and use information.' Third, 'Information operations refer to a series of operational actions undertaken to gain and maintain information superiority on the battlefield or control over information. The two sides in a conflict use electronic warfare or computer network warfare to use or destroy the information and information networks of the enemy and protect one's own information networks as a means of acquiring, controlling, and using information.

Clearly, the targets of information operations are information itself, information systems, as well as peoples' cognition and beliefs. IO means employed include information (both information media and information content) and weapons and equipment dedicated for attacks on information systems. Information operations involve both attacking and defending.

Dai and his co-workers added one more definition of IO in this book. The description lists the targets of IO and the means employed, stating:

Information operations are defined as a series of countermeasures employed by two sides in a conflict in which information or weapons and equipment controlled by information and dedicated to the destruction of information systems are used in order to influence and destroy the enemy's information, information systems, and cognition and beliefs, along with preventing the influence and destruction of one's own information,

information systems, and cognition and beliefs in the same manner by an enemy.

China's emphasis on countermeasures is a significant deviation from Western definitions. When the PRC collects technical parameters of other systems, they develop countermeasures as a sort of asymmetric response. China's 2006 White Paper, when discussing army projects, noted information countermeasure units were one of three organizations requiring priority development. The primary reason behind this force may be to construct IW countermeasures.

Neutralizing the Internet Against Extremism

China's police are starting to use cartoon police characters on domestic Internet sites to warn users against using illegal content. At the moment these friendly looking male and female cartoon character alerts walk, bike, or drive across the screen at half hour intervals on 13 of China's most popular portals. According to the Beijing Public Security Ministry, these virtual police are expected to populate all registered websites in China in 2008.

While these animations warn users that someone is watching, such warnings are a far cry from neutralizing an extremist's use of the Internet. With 137 million users at present, and an Internet population expected to surpass the US in two years, the challenge could be a stiff one. The common tactic is to simply close down domestic websites deemed extremist or subversive or to intercept emails with words like "Falun Gong" or the "Dalai Lama." Email services in China are obligated to hand over user data and communications to Chinese security officials if asked for such material, which is another way to help neutralize an extremist's use of the Web.

In order to stem the tide of Internet crime, China reportedly increased the size of its Internet police force in 2000 to some 300,000 personnel. While this figure is difficult to comprehend, these crime fighters are part of the Ministry of Public Security and, thus, may have jobs other than fighting crime (espionage, etc.). The Internet police are mainly responsible for carrying out supervision, analyzing information content flowing through local communication systems or the Internet, fighting computer viruses, cracking down on Internet crimes, and stopping the spread of "harmful information." It is the influence of the latter, of—the extremists and nationalists—that China wants to limit inside its borders. However, very little has been written in China on the Internet war in Iraq, and the fight against extremism worldwide.

China wants to make this a joint effort. Reserve, militia, PLA, and civilian forces are conducting joint operations against notional intervening IW forces. This integration is underway in the form of a proposed a 'cyber security force' (CSF). Qu Yanwen, a security specialist, proposes a unit composed of members of the PLA, the Ministries of State Security and Public Security, and technical specialists. Local authorities state Chinese political, economic, and military security is in danger due to the nascent stage of development of China's networks. Weaknesses exist in financial security; in defending against cyber attacks against information networks of key organizations and computer-based fund raising operations and scams; in information control over data that can affect the stability of public order; and in military information security. Within the PLA, the Shijiazhuang Army Command College, the Navy Command Academy, the Air Force Command Academy, and the Second Artillery Corps Command Academy met in July 2007 to work out an overall joint teaching program for the three armed forces. They are trying to share information resources and exchange experiences via the Internet, among other issues.

The People's Republic of China in its Asian context. (Wikimedia)

According to one report, arrests and prosecutions for endangering state security have risen sharply overall since 11 September 2001. In the two-year period ending 31 December 2002, more than 1,600 people were prosecuted for endangering state security, most after the terror attacks on the US. Many of those arrested and prosecuted hail from Xinjiang, which Chinese sources characterize as an autonomous region in the northwest of the country, that is home to a large and restive Muslim population. China's government has used the war on terror to crack down on those seeking greater autonomy, including those who do so by peaceful means.

What we do know about the domestic population arrested for political crimes is of interest. John Kamm, President of the Dui Hua Foundation ("dui hua "means "dialogue" in Mandarin Chinese, and is a non-profit, human rights organization), wrote that about one-quarter of those arrested are non-Han Chinese, principally Tibetans and Uyghurs. Since China is more than 90% Han, the number of non-Han arrests is well out of proportion to the rest of the population. Kamm writes that sentences for non-Han Chinese are typically longer than those imposed on Han Chinese. With some candor, China's government recently released statistics on people arrested and prosecuted for endangering state security, the most serious political offence in the criminal code. China's top prosecutor, Han Zhubin, revealed that more than 3,400 people were arrested from 1998 to 2002 for such crimes as subversion, incitement to subversion, espionage, and trafficking in state

secrets. Kamm adds that "Internet dissidents" make up the fastest-growing group of political prisoners.

China has been concerned about Internet political movement activities since at least 1996. In that year the East Turkistan information Center (ETIC) was formed, operating out of Munich, Germany. This site now delivers news to 114 countries in seven languages, and focuses on news, both positive and negative, about the Uyghur cause. Calling Chinese Communists "fascist authorities," the website covers incidents reportedly aimed at robbing the Uyghur culture of its ideological roots, via a massive reeducation campaign. In 2004 ETIC also established a Uyghur Internet TV station.

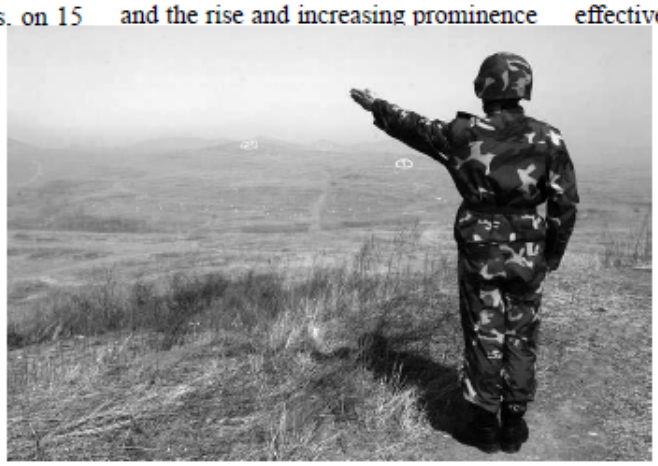
In response to these events, on 15 December 2003 the *Beijing Xinhua* news service reported that China's Ministry of Public Security identified the East Turkistan Information Center as a terrorist organization and its director, Abudujelili Kalakash, as a terrorist. A week later, the East Turkistan Information Center offered to disband, if the communist state offered freedom of expression and Internet access to Uyghur Muslim minorities. In 2005, a Beijing Communist Youth newspaper, *Zhongguo Qingnian Bao*, identified East Turkistan terrorist forces as the main terrorist threat to China.

The battle for control of the news has not stopped. China reported on an incident in January 2007 and provided its version of a scuffle between the PLA and "ethnic militants." ETIC's website reported the conflict occurred in a different area than that reported by Chinese TV, and that more PLA servicemen died than was reported by Chinese authorities.

What is Special About Chinese IO?

The key to understanding the Chinese approach to IO consists of two unique and noteworthy issues. The first is the extent to which the Chinese integrate strategy with IO. The second related issue is the focus on countermeasures and reconnaissance.

Peng Guangqian and Yao Youzhi, editors of the popular Chinese book *The Science of Military Strategy*, note that the PLA must be "guided by the principles of military strategy in the new era to bring forth new ideas to push ahead the principles of strategic actions for local war under high-tech conditions…" This strategy-IO or strategy-technology integration was also highlighted by other authors. Perhaps the most notable comments were made by IW specialists Shen Weiguang and Dai Qingmin. Shen, the reputed father of information warfare in China, notes "The issue of information and network security, which accompanies the development of informationization, and the rise and increasing prominence of information warfare, the form of warfare that is invisible and non-violent, is an issue of technology, **but above all else it is an issue of strategy**."



People's Liberation Army colonel points the way. (Defense Link)

Major General Dai Qingmin, the former head of the information warfare directorate of the Chinese General Staff, offered a similar statement about the importance and probability of an IW/IO-strategic integration. He notes:

Laying all one's hopes on technology is dangerous. The road to future losses may not be from a fall in technology, it may be primarily poor strategy. In reality the informationization of the forms of warfare has opened up an even broader space for playing tricks and using strategy and for using the indirect to gain the upper hand.

According to Shen and Dai, even conditions of technological superiority will not allow for success in all cases, if one overlooks strategy.

IO provides the PLA with a new means for applying strategy, one that enables a new information-based use of manipulation, deception, and soft (computer) destruction as much as hard (physical) destruction. Noted Chinese strategist Li Bingyan offered three observations: first, that collecting too much information can be blinding and can prohibit or stilt strategy; second, that weak information technology nations can successfully attack strong information technology nations with the use of stratagems; and third, that information technology can serve strategy as an effective deterrent and prevent war from ever breaking out (the Chinese think the use of information technology at the Dayton talks to end the war in the former Yugoslavia is a prime example of winning without fighting). These are direct examples of how IO and strategy are being integrated into Chinese thinking.

Peng and Yao offer other strategy-IO paradigms in *The Science of Military Strategy*. They write about the strategic maneuver aspect of strategy's applied theory, and stating the struggle in the information field may lead to changes in strategic maneuver. In particular, a "strategic information operations force may become a new form of strategic maneuver in future wars." If such a type of maneuver actually does develop, then IO experts must also explore questions in the applied theory arena. Will there be cyberflanking, cyberpenetration, and other cyber activities? One would think so, based articles that have appeared in authoritative Chinese military journals.

The second special issue after the strategy-IO link is China's focus on countermeasures and reconnaissance. By collecting technical parameters of other systems, China can use them to construct countermeasures, as a sort of asymmetric response.

The Chinese note that the US launched reconnaissance in the form of electronic warfare and intelligence warfare more than six months before the First Gulf War began. Such US actions are in line with Sun Tzu's concept that "the clever combatant seeks battle after the victory has been won." Chinese theorists have certainly bought into this concept of reconnaissance and intelligence warfare well before a battle begins. According to General Dai, China's vision of future war first involves information reconnaissance, to collect technical parameters. This will ensure victory before the first battle. Reconnaissance (consisting of electronic warfare, radar, radio technology, and network reconnaissance) fits perfectly with Dai's and Sun Tzu's concepts and stratagem.

Dai's writings focus not only on collecting technical parameters, specific properties of information weapon systems and electronic information products, but also on information attacks. This implies that collecting parameters and performing reconnaissance are two prerequisites for preemptive attacks. Computer network reconnaissance helps choose which opportune moments, which places, and which attack measures will result in maximum success—if war ever breaks out. Peng and Yao seconded this concept, stating that IO is directly linked to the gain or loss of the initiative in war and thus "priority should be given to the attack and combining the attack with the defense." Thus it appears information technology has enhanced Chinese thinking with regard to preemption. Chinese military academics state that those who do not preempt lose the initiative, in what may be a very short-lived IO war.

Conclusion

Combatants in present day conflicts may find it easier than at any other time in history to obtain their wartime objectives through one campaign, or one battle in the IO age. The idea of sudden attack has changed, especially if one side possesses high-technology equipment and the other side only low-technology means, which allows for better reconnaissance and insertion of preemptive mechanisms (back doors in computer programs, etc.). "Attack" doesn't mean "surprise" in the old sense, but rather that one side can't correspondingly react if they're aware of the enemy situation. You may know where all of the forces are on the enemy side, yet your systems can't respond due to preemptive computer measures an enemy has taken in peacetime. If war does break out, then preemptive attacks focus on "striking the enemy's information center of gravity and weakening the combat efficiency of his information systems and cyberized weapons." This allows one to weaken the enemy's information superiority and reduce his holistic combat efficiency.

Perhaps the current emphasis on gaining the initiative, and on short wars that are over quickly, are the main reasons that Dai gives the impression that preemption is a necessity, noting:

Actions such as intelligence warfare, psychological warfare, and campaign deception in advance of combat seem to be even more important to the unimpeded implementation of planning and ensuring war. For this reason, information warfare must be started in advance of other combat actions before making war plans and while making war plans.

In a sense, it is the special features of IO tactics and techniques that enable the increased emphasis on cyber attacks more than traditional ground, sea, or air warfare. For example, a weaker force can inflict much damage on a superior force with a properly timed and precisely defined asymmetric information attack. Such an offensive may be impossible by traditional means. Multiple information attack actions can be developed, the offense considered as defense, and information barrier methods developed—by both strong and weak opponents. Attack tactics include information deterrence, information blockade, information power creation (electronic camouflage, network deception, etc.), information contamination, information harassment, nodal destruction, system paralysis, and entity destruction.

China's specific understanding of the intersection of strategy and information technology, especially as it relates to conflict, is not based on a wartime scenario in a practical sense; China lacks recent combat experience. However, from a theoretical perspective and use of IO techniques in peacetime, China has written extensively on the use of information technology and preemption. Based on the number of attacks worldwide attributed to China, they have given much thought to these issues, and apparently have some recent practical experience.

Timothy L. Thomas is a senior analyst at the Foreign Military Studies Office (FMSO) at Fort Leavenworth, Kansas. Mr. Thomas received a BS from West Point and an MA from the University of Southern California. He was a US Army Foreign Area Officer who specialized in Soviet/Russian studies. His military assignments included serving as the Director of Soviet Studies at the United States Army Russian Institute (USARI) in Garmisch, Germany; as an inspector of Soviet tactical operations under CSCE; and as a Brigade S-2 and company commander in the 82nd Airborne Division. He is an adjunct professor at the US Army's Eurasian Institute; an adjunct lecturer at the USAF Special Operations School; and a member of two Russian organizations, the Academy of International Information, and the Academy of Natural Sciences.